



**State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory**

**December 19, 2007**

*The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**STATE OF ALASKA ADVISORY NUMBER:**

2007-027

**DATE ISSUED:**

December 19, 2007

**SUBJECT:**

Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Adobe Flash Player. These vulnerabilities can be exploited if a user visits a website hosting the malicious content or opens a malicious Flash file. If the vulnerability is successfully exploited, the attacker will have the same rights as the logged on user. This may allow the attacker to take complete control of the affected system.

It should be noted that Adobe Flash Player is installed on most of the systems where web browsers are used to access the Internet.

**SYSTEMS AFFECTED:**

- Adobe Flash Player 7.0.69.0
- Adobe Flash Player 8.0.34.0
- Adobe Flash Player 9.0.28.0
- Adobe Flash Player 9.0.31.0
- Adobe Flash Player 9.0.45.0
- Adobe Flash Player 9.0.47.0
- Adobe Flash Player 9.0.48.0
- RedHat Enterprise Linux Desktop Supplementary v.5 client
- RedHat Enterprise Linux Extras 4.5.z
- RedHat Enterprise Linux Extras v.3
- RedHat Enterprise Linux Extras v.4
  - RedHat Enterprise Linux Supplementary v.5 server

**RISK:**

**Government:**

Large and medium government entities: **High**

Small government entities: **High**

**Businesses:**

Large and medium business entities: **High**

Small business entities: **High**

**Home users: High**

**DESCRIPTION:**

Multiple vulnerabilities have been discovered in Adobe Flash Player which could allow attackers to execute arbitrary code, and/or misrepresent how webpages are interpreted on affected systems.

Vulnerable systems can be exploited if a user visits a malicious web page or manually opens a malicious .swf file. An attacker who exploits this vulnerability will gain the same privileges as the logged on user. If the user account is configured with administrative privileges, successful exploitation will result in attacker taking complete control of an affected system. This could allow the attacker to install programs; add, view or delete user data; or create new accounts.

Adobe Flash Player is installed on many Microsoft Windows, Mac OSX, and Linux/UNIX workstations since many web applications use it for frame-based animations with sound to be viewed within a web browser. Therefore, wide spread use of this application coupled with limited user interaction required for exploitation increases the criticality of this vulnerability.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply the appropriate update to vulnerable systems immediately after appropriate testing.
- Logon to your systems as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. Employ the principle of least privilege when ever possible.
- Do not open email attachments, including media content, from untrusted sources.
- Do not visit unknown or un-trusted Web sites or click on links provided in an email.

**REFERENCES:**

**Adobe:**

<http://www.adobe.com/support/security/bulletins/apsb07-20.html>

<http://www.adobe.com/products/flash/>

**Red Hat:**

<https://rhn.redhat.com/errata/RHSA-2007-1126.html>

**Security Focus:**

<http://www.securityfocus.com/bid/26929>

**US-CERT:**

<http://www.kb.cert.org/vuls/id/945060>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6242>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4768>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5275>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6243>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6244>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6245>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4324>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6246>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5476>